



EIGRP

이 섹션에서는 데이터 라우팅, 인증 수행, 라우팅 정보 재배포를 위해 EIGRP(Enhanced Interior Gateway Routing Protocol)를 사용하여 threat defense를 구성하는 방법을 설명합니다.

- [EIGRP 라우팅 정보, 1 페이지](#)
- [EIGRP의 시스템 요구 사항 및 사전 요건, 2 페이지](#)
- [EIGRP 라우팅에 대한 지침 및 제한 사항, 3 페이지](#)
- [EIGRP 구성, 4 페이지](#)
- [EIGRP 기록, 11 페이지](#)

EIGRP 라우팅 정보

Cisco에서 개발한 EIGRP(Enhanced Interior Gateway Routing Protocol)는 IGRP의 향상된 버전입니다. IGRP 및 RIP와 달리 EIGRP는 주기적인 경로 업데이트를 전송하지 않습니다. EIGRP 업데이트는 네트워크 토폴로지가 변경될 때만 전송됩니다. EIGRP를 다른 라우팅 프로토콜과 차별화하는 핵심 기능으로는 빠른 컨버전스, variable-length 서브넷 마스크 지원, 부분 업데이트 지원, 다중 네트워크 계층 프로토콜 지원이 있습니다.

EIGRP를 실행하는 라우터는 모든 네이버 라우팅 테이블을 저장하여 다른 경로에 빠르게 적응할 수 있습니다. 적절한 경로가 존재하지 않는 경우 EIGRP는 네이버를 쿼리하여 대체 경로를 찾습니다. 이 쿼리는 대체 경로를 발견할 때까지 전파됩니다. EIGRP는 variable-length 서브넷 마스크 지원을 통해 네트워크 경계에서 경로를 자동으로 요약할 수 있습니다. 또한 EIGRP는 모든 인터페이스의 모든 비트 경계에서 요약되도록 구성할 수 있습니다.

EIGRP는 주기적인 업데이트를 만들지 않습니다. 대신 경로의 메트릭이 변경될 때 부분적인 업데이트를 전송합니다. 부분 업데이트 전파가 자동으로 바운딩되므로 정보가 필요한 라우터만 업데이트됩니다. 이 두 기능 덕분에 EIGRP는 IGRP보다 훨씬 적은 대역폭을 사용합니다.

직접 연결된 네트워크의 다른 라우터를 동적으로 학습하기 위해 위협 방어는 인접 라우터 검색을 사용합니다. EIGRP 라우터는 멀티캐스트 hello 패킷을 전송하여 네트워크에서 존재를 알립니다. EIGRP 디바이스가 새로운 네이버에서 hello 패킷을 수신하면 초기화 비트 세트와 함께 토폴로지 테이블을 네이버로 보냅니다. 초기화 비트 세트와 함께 토폴로지 업데이트를 수신한 네이버는 토폴로지 테이블을 다시 디바이스로 전달합니다.

hello 패킷은 멀티캐스트 메시지로 전달됩니다. hello 메시지에는 응답할 필요가 없습니다. 고적으로 정의된 인접 라우터는 이 규칙의 예외입니다. 네이버를 수동으로 구성하는 경우, hello 메시지, 라우팅 업데이트 및 승인은 유니캐스트 메시지로 전송됩니다.

이 네이버 관계가 설정되면 네트워크 토폴로지의 변화가 없는 한 라우팅 업데이트가 교환되지 않습니다. 네이버 관계는 hello 패킷을 통해 유지됩니다. 네이버에서 수신된 각 hello 패킷은 보류 시간을 포함합니다. 보류 시간은 위협 방어가 해당 네이버로부터 hello 패킷을 수신할 것으로 예상할 수 있는 시간입니다. 디바이스가 해당 인접 디바이스가 알린 보류 시간 내에 인접 디바이스로부터 hello 패킷을 수신하지 않으면 디바이스는 해당 인접 디바이스를 사용할 수 없는 것으로 간주합니다.

EIGRP는 경로 계산에 인접 디바이스 검색/복구, RTP(Reliable Transport Protocol) 및 DUAL(Diffusing Update Algorithm)을 사용합니다. DUAL은 least-cost 경로뿐 아니라 토폴로지 테이블의 대상에 대한 모든 경로를 저장합니다. least-cost 경로가 라우팅 테이블로 삽입됩니다. 다른 경로는 토폴로지 테이블에 남아 있습니다. 기본 경로가 실패할 경우 가능한 successor에서 다른 경로가 선택됩니다. successor는 대상에 대한 least-cost 경로를 가진 패킷 전달에 사용되는 네이버 라우터입니다. 가능성 계산은 경로가 라우팅 루프의 일부가 아님을 보장합니다.

토폴로지 테이블에서 가능한 successor를 찾을 수 없는 경우 경로 재계산이 이루어집니다. 경로 재계산 중에 DUAL은 EIGRP 네이버에 경로를 쿼리합니다. 쿼리는 연속 인접 항목으로 전파됩니다. 적합한 후속 작업을 찾을 수 없는 경우 연결할 수 없다는 메시지가 반환됩니다.

경로 재계산 중 DUAL은 경로를 활성으로 표시합니다. 기본적으로 위협 방어는 인접 디바이스로부터 응답을 수신하기 위해 3분을 대기합니다. 디바이스가 인접 디바이스로부터 응답을 수신하지 않는 경우 경로가 stuck-in-active로 표시됩니다. 가능한 successor로서 응답이 없는 네이버를 가리키는 토폴로지 테이블의 모든 경로는 제거됩니다.

EIGRP의 시스템 요구 사항 및 사전 요건

모델 지원

Threat Defense

Threat Defense Virtual

지원되는 도메인

모두

사용자 역할

관리자

네트워크 관리자

EIGRP 라우팅에 대한 지침 및 제한 사항

방화벽 모드 지침

라우팅된 방화벽 모드에서만 지원됩니다.

디바이스 지침

- 디바이스당 하나의 EIGRP 프로세스만 허용됩니다.
- EIGRP는 threat defense 6.6 이상 버전에서 관리 센터 UI를 통해 구성할 수 있습니다.

인터페이스 지침

- 논리적 이름이 있고 IP 주소가 있는 라우팅된 인터페이스만 EIGRP 라우팅 프로세스와 연결할 수 있습니다.
- 전역 가상 라우터에 속한 인터페이스만 EIGRP의 일부가 될 수 있습니다. EIGRP는 글로벌 가상 라우터의 라우팅 프로토콜을 통해 경로를 학습, 필터링 및 재배포할 수 있습니다.
- 물리적, EtherChannel, 이중, 하위 인터페이스만 지원합니다. 그러나 EtherChannel 인터페이스의 멤버는 지원되지 않습니다.
- BVI 및 VNI는 EIGRP의 일부가 될 수 없습니다.
- 패시브 인터페이스는 네이버 인터페이스로 구성할 수 없습니다.

IP 주소 및 네트워크 개체 지원

- IPv4 주소만 지원됩니다.
- 범위, FQDN 및 와일드카드 마스크는 지원되지 않습니다.
- 표준 액세스 목록 개체만 지원됩니다.

재배포 지침

- 글로벌 가상 라우터의 BGP, OSPF 및 RIP는 EIGRP에 재배포할 수 있습니다.
- EIGRP는 글로벌 가상 라우터에서 BGP, OSPF, RIP, Static 및 Connected에 재배포할 수 있습니다.
- OSPF 네트워크에 속한 디바이스에 EIGRP가 구성되어 있거나 그 반대의 경우, OSPF 라우터가 경로에 태그를 지정하도록 구성하십시오(EIGRP는 경로 태그를 지원하지 않음).

EIGRP를 OSPF로, OSPF를 EIGRP로 재배포할 때 링크 또는 인터페이스 중 하나에서 중단이 발생하거나 경로 발신자가 다운된 경우에도 라우팅 루프가 발생합니다. 한 도메인의 경로가 동일한 도메인으로 다시 재배포되는 것을 방지하기 위해 라우터는 재배포하는 동안 도메인에 속한 경로에 태그를 지정할 수 있으며, 이러한 경로는 동일한 태그를 기반으로 원격 라우터에서 필터

링될 수 있습니다. 경로는 라우팅 테이블에 설치되지 않으므로 동일한 도메인으로 다시 재배포되지 않습니다.

구축 프로세스 지침

구축된 EIGRP 구성의 기존 AS 번호를 변경하려면 EIGRP를 비활성화하고 구축해야 합니다. 이 단계에서는 위협 방어에 구축된 EIGRP 구성을 지웁니다. 다음으로, 새 AS 번호를 사용하여 EIGRP 구성을 다시 생성한 다음 구축합니다. 따라서 이 프로세스는 위협 방어에 구축되는 동일한 EIGRP 구성으로 인해 구축 실패를 방지합니다.

업그레이드 지침

이전 버전에 FlexConfig EIGRP 정책이 있을 때 버전 7.2 이상으로 업그레이드하면 구축 중에 관리 센터에 경고 메시지가 표시됩니다. 그러나 구축 프로세스는 중지되지 않습니다. 그러나 구축 후에 UI(**Device (Edit)**(디바이스(편집)) > **Routing**(라우팅) > **EIGRP**)에서 EIGRP 정책을 관리하려면 **Device (Edit)**(디바이스(편집)) > **Routing**(라우팅) > **EIGRP** 페이지에서 구성을 다시 실행하고 FlexConfig에서 구성을 제거해야 합니다. UI에서 정책 생성을 자동화하기 위해 management center는 FlexConfig에서 UI로 정책을 마이그레이션하는 옵션을 제공합니다. 자세한 내용은 [FlexConfig 정책 마이그레이션](#)을 참조하십시오.

EIGRP 구성

Routing(라우팅) 탭에서 방화벽 디바이스에 대해 EIGRP를 활성화하고 구성할 수 있습니다.

프로시저

- 단계 1 **Devices**(디바이스) > **Device Management**(디바이스 관리)를 선택하고 threat defense 디바이스를 편집합니다.
- 단계 2 라우팅 탭을 클릭합니다.
- 단계 3 Global(전역) 아래에서 **EIGRP**를 클릭합니다.
- 단계 4 EIGRP 라우팅 프로세스를 활성화하려면 **Enable EIGRP**(EIGRP 활성화) 체크 박스를 선택합니다.
- 단계 5 **AS Number**(AS 번호) 필드에 EIGRP 프로세스에 대한 자율 시스템(AS) 번호를 입력합니다. AS 번호는 여러 자율 번호를 포함합니다. AS 번호는 1부터 65535까지 사용할 수 있으며 인터넷에서 각 네트워크를 식별하는 고유 할당 값입니다.
- 단계 6 다른 EIGRP 속성을 구성하려면 다음 주제를 참조하십시오.
 1. [EIGRP 설정 구성, 5 페이지](#).
 2. [EIGRP 인접한 라우터 설정 구성, 5 페이지](#).
 3. [EIGRP 필터 규칙 구성, 6 페이지](#).
 4. [EIGRP 재배포 설정 구성, 6 페이지](#).
 5. [EIGRP 요약 주소 설정 구성, 8 페이지](#).

6. EIGRP 인터페이스 설정 구성, 8 페이지.
7. EIGRP 고급 설정 구성, 9 페이지.

EIGRP 설정 구성

프로시저

- 단계 1 **EIGRP** 페이지에서 **Setup**(설정) 탭을 클릭합니다.
- 단계 2 네트워크 번호 경계를 요약하도록 EIGRP를 활성화하려면 **Auto Summary**(자동 요약) 체크 박스를 선택합니다.
- 참고 자동 요약을 활성화하면 불연속 네트워크를 가진 경우 라우팅 문제가 발생할 수 있습니다.
- 단계 3 **Available Networks/Hosts**(사용 가능한 네트워크/호스트) 상자에서 EIGRP 라우팅 프로세스에 참여해야 하는 네트워크 또는 호스트를 클릭한 다음 **Add**(추가)를 클릭합니다. 네트워크 개체를 새로 추가하려면 **Add**(추가) (+)을 클릭합니다. 네트워크 추가 절차는 **네트워크**의 내용을 참조하십시오.
- 단계 4 패시브 인터페이스를 구성하려면 **Passive Interface**(패시브 인터페이스) 체크 박스를 선택합니다. EIGRP에서 패시브 인터페이스는 라우팅 업데이트를 보내거나 받지 않습니다.
- a) 선택적 인터페이스를 패시브로 지정하려면 **Selected Interface**(선택한 인터페이스) 라디오 버튼을 클릭합니다. **Available Interfaces**(사용 가능한 인터페이스) 상자에서 인터페이스를 선택하고 **Add**(추가)를 클릭합니다.
 - b) 모든 인터페이스를 패시브로 지정하려면 **All Interfaces**(모든 인터페이스) 라디오 버튼을 클릭합니다.
- 단계 5 **Ok**(확인)를 클릭하고 설정을 **Save**(저장)합니다.

EIGRP 인접한 라우터 설정 구성

EIGRP 프로세스에 대한 고정 인접 디바이스를 정의할 수 있습니다. EIGRP 인접한 라우터를 수동으로 정의할 경우 hello 해당 인접한 라우터로 유니캐스트됩니다.

프로시저

- 단계 1 **EIGRP** 페이지에서 **Neighbors**(인접한 라우터) 탭을 클릭합니다.
- 단계 2 **Add**(추가)를 클릭합니다.
- 단계 3 **Interface**(인터페이스) 드롭다운 목록에서 인접한 라우터가 제공되는 인터페이스를 선택합니다.

단계 4 **Neighbor**(인접한 라우터) 드롭다운에서 고정 인접한 라우터의 IP 주소를 선택합니다. 네트워크 개체를 추가하려면 **Add**(추가) (+)을 클릭합니다. 네트워크 개체 추가 절차는 [네트워크](#)의 내용을 참조하십시오.

단계 5 **Ok**(확인)를 클릭하고 설정을 **Save**(저장)합니다.

EIGRP 필터 규칙 구성

EIGRP 라우팅 프로세스에 대한 경로 필터링 규칙을 구성할 수 있습니다. 필터 규칙을 통해 EIGRP 라우팅 프로세스가 수락하거나 알리는 경로를 제어할 수 있습니다.

프로시저

단계 1 **EIGRP** 페이지에서 **Filter Rules**(필터 규칙) 탭을 클릭합니다.

단계 2 **Add**(추가) (+) 버튼을 클릭합니다.

단계 3 **Add Filter Rules**(필터 규칙 추가) 대화 상자의 **Filter Direction**(필터 방향) 드롭다운에서 규칙의 방향을 선택합니다.

- **Inbound**(인바운드)—규칙이 수신 EIGRP 라우팅 업데이트에서 기본 경로 정보를 필터링합니다.
- **Outbound**(아웃바운드)—규칙이 발신 EIGRP 라우팅 업데이트에서 기본 경로 정보를 필터링합니다.

단계 4 필터링 규칙을 적용할 인터페이스를 선택하려면 **Interface**(인터페이스) 라디오 버튼을 클릭하고 드롭다운에서 인터페이스를 선택합니다.

단계 5 필터링 규칙을 적용할 프로토콜을 선택하려면 **Protocol**(프로토콜) 라디오 버튼을 클릭하고 드롭다운에서 프로토콜(**BGP**, **RIP**, **Static**, **Connected** 또는 **OSPF**)을 선택합니다. **BGP** 및 **OSPF** 프로토콜의 경우 관련 프로세스 ID를 지정할 수 있습니다.

단계 6 **Access List**(액세스 목록) 드롭다운 목록에서 액세스 목록을 선택합니다. 목록은 라우팅 업데이트에서 어떤 네트워크를 수신하고 어떤 네트워크를 억제할지 정의합니다. 새 표준 액세스 목록 개체를 추가하려면 **Add**(추가) (+)을 클릭합니다. 자세한 절차는 [표준 ACL 개체 설정](#)의 내용을 참조하십시오.

단계 7 **Ok**(확인)를 클릭하고 설정을 **Save**(저장)합니다.

EIGRP 재배포 설정 구성

다른 라우팅 프로토콜에서 EIGRP 라우팅 프로세스로 경로를 재배포하기 위한 규칙을 정의할 수 있습니다.

프로시저

단계 1 **EIGRP** 페이지에서 **Redistribution**(재배포) 탭을 클릭합니다.

단계 2 **Add**(추가) (+) 버튼을 클릭합니다.

단계 3 **Add Redistribution**(재배포 추가) 대화 상자의 **Protocol**(프로토콜) 드롭다운 목록에서 경로가 재분배될 소스 프로토콜을 선택합니다.

- BGP - BGP 라우팅 프로세스에서 검색된 경로를 EIGRP로 재배포합니다.
- RIP - RIP 라우팅 프로세스에서 검색된 경로를 EIGRP로 재배포합니다.
- Static(고정) - 고정 경로를 EIGRP 라우팅 프로세스로 재배포합니다. 네트워크 구문 범위에 해당하는 고정 경로는 EIGRP로 자동으로 재배포됩니다. 이에 대한 재배포 규칙을 정의할 필요가 없습니다.
- Connected(연결됨) — 연결된 경로(인터페이스에서 IP 주소를 활성화하여 자동으로 설정된 경로)를 OSPF 연결 프로세스에 재배포합니다. 네트워크 구문 범위에 해당하는 연결된 경로는 EIGRP로 자동으로 재배포됩니다. 이에 대한 재배포 규칙을 정의할 필요가 없습니다.
- OSPF - OSPF 라우팅 프로세스에서 검색된 경로를 EIGRP로 재배포합니다. 이 프로토콜을 선택하는 경우, 이 대화상자의 Match(일치) 옵션은 선택적 **OSPF** 재배포에서 사용할 수 있습니다.
 - Internal(내부) — 특정 AS 시스템의 내부 경로입니다.
 - External 1(외부 1) — AS의 외부에 있지만, OSPF에 Type 1 외부 경로로서 가져온 경로입니다.
 - External2(외부 2) - AS의 외부에 있으며 선택한 프로세스에 Type 2 외부 경로로 가져온 경로입니다.
 - Nsaa-External1 - AS 외부에 있으며 Type 1 외부 경로로 선택한 프로세스에 가져온 NSSA(Not-So-Stubby Area) 경로입니다.
 - Nsaa-External2 - AS 외부에 있으며 Type 2 외부 경로로 선택한 프로세스에 가져온 (NSSA) 경로입니다.

참고 고정 경로, 연결된 경로, RIP 또는 BGP 경로를 재배포할 경우 이러한 옵션이 제공되지 않습니다.

단계 4 **Optional Metrics**(선택적 메트릭)에서 관련 값을 입력합니다.

- **Bandwidth**(대역폭) — 경로의 최소 대역폭(초당 킬로 비트)입니다. 유효한 값의 범위는 1 ~ 4294967295입니다.
- **Delay Time**(지연 시간) — 10마이크로초 단위의 경로 지연입니다. 유효한 값의 범위는 0 ~ 4294967295입니다.
- **Reliability**(신뢰성) — 패킷 전송의 성공률이며 0~255의 숫자로 표시됩니다. 값 255는 100% 신뢰성을 나타내고, 0은 신뢰성 없음을 의미합니다.

- **Loading(로딩)**—경로의 유효 대역폭입니다. 유효한 값의 범위는 1 ~ 255입니다. 255는 100% 로딩을 나타냅니다.
- **MTU**— 경로의 최대 전송 단위에 허용되는 최소 값입니다. 유효한 값의 범위는 1 ~ 65535입니다.

단계 5 **Route Map**(경로 맵) 드롭다운 목록에서 재배포 항목에 적용할 경로 맵 개체를 선택합니다. 새 경로 맵 개체를 생성하려면 **Add(추가)** (+)를 클릭합니다. 새 경로 맵을 추가하는 절차는 [경로 맵 항목 구성](#)을 참조하십시오.

단계 6 **Ok(확인)**를 클릭하고 설정을 **Save(저장)**합니다.

EIGRP 요약 주소 설정 구성

각 인터페이스에 대한 요약 주소를 구성할 수 있습니다. 네트워크 경계에서 발생하지 않는 요약 주소를 생성하려는 경우 또는 자동 경로 요약을 비활성화하고 위협 방어에서 요약 주소를 사용하려는 경우 요약 주소를 수동으로 정의해야 합니다. 라우팅 테이블에 다른 특정 경로가 있는 경우 EIGRP는 모든 추가 경로의 최소값과 동등한 메트릭을 통해 요약 주소를 알립니다.

프로시저

단계 1 **EIGRP** 페이지에서 **Summary Address**(요약 주소) 탭을 클릭합니다.

단계 2 **Add(추가)**를 클릭합니다.

단계 3 **Interface**(인터페이스) 드롭다운에서 요약 주소를 알릴 인터페이스를 선택합니다.

단계 4 **Network**(네트워크) 드롭다운에서 요약할 특정 IP 주소 및 네트워크 마스크가 있는 네트워크 개체를 선택합니다. 새 네트워크를 추가하려면 **Add(추가)** (+)을 클릭합니다. 네트워크 추가 절차는 [네트워크](#)의 내용을 참조하십시오.

단계 5 **Administrative Distance**(관리 거리) 필드에 요약 경로의 관리 거리를 입력합니다. 유효한 값의 범위는 1 ~ 255입니다.

단계 6 **Ok(확인)**를 클릭하고 설정을 **Save(저장)**합니다.

EIGRP 인터페이스 설정 구성

Interfaces(인터페이스) 탭에서 인터페이스별 EIGRP 라우팅 속성을 구성할 수 있습니다.

프로시저

단계 1 **EIGRP** 페이지에서 **Interfaces**(인터페이스) 탭을 클릭합니다.

단계 2 **Add(추가)** (+) 버튼을 클릭합니다.

- 단계 3 **Interface**(인터페이스) 드롭다운에서 구성이 적용되는 인터페이스의 이름을 선택합니다.
- 단계 4 **Hello Interval(Hello 간격)** 필드에 인터페이스에서 EIGRP hello 패킷이 전송되는 간격(초)을 입력합니다. 유효한 값의 범위는 1 ~ 65535입니다. 기본값은 5초입니다.
- 단계 5 **Hold Time**(보류 시간) 필드에 EIGRP hello 패킷에서 디바이스가 알리는 보류 시간을 입력합니다. 유효한 값의 범위는 3 ~ 65535입니다. 기본값은 180초입니다.
- 단계 6 인터페이스에서 EIGRP 분할-수평을 활성화하려면 **Split Horizon**(수평 분할) 확인란을 클릭합니다.
- 단계 7 **Delay Time**(지연 시간) 필드에 10마이크로초 단위로 지연 시간을 입력합니다. 유효한 값은 1 ~ 16777215입니다. 이 옵션은 다중 상황 모드의 디바이스에서 지원되지 않습니다.
- 단계 8 **Authentication**(인증) 속성에 대한 값을 지정합니다.
- **Enable MD5 Authentication(MD5 인증 활성화)** - EIGRP 패킷 인증에 MD5 해시 알고리즘을 사용하려면 이 체크 박스를 선택합니다.
 - **Key Type**(키 유형) - 드롭다운에서 다음 키 유형 중 하나를 선택합니다.
 - **None**(없음) - 인증이 필요하지 않음을 나타냅니다.
 - **Unencrypted**(암호화되지 않음) - 인증에 사용할 키 문자열이 일반 텍스트 비밀번호임을 나타냅니다.
 - **Encrypted**(암호화됨) - 사용할 키 문자열이 인증에 암호화된 비밀번호임을 나타냅니다.
 - **Auth Key**(인증 키) - 사용할 키 문자열이 EIGRP 인증 키임을 나타냅니다.
 - **Key ID**(키 ID) — EIGRP 업데이트를 인증하는 데 사용되는 키의 ID입니다. 숫자 키 식별자를 입력합니다. 유효한 값의 범위는 0 ~ 255입니다.
 - **Key**(키) — 최대 17자의 영숫자 문자열입니다. 암호화된 인증 유형의 경우 이 필드는 17자 이상이어야 합니다.
 - **Confirm Key**(키 확인) - 키를 다시 입력합니다.
- 단계 9 **Ok**(확인)를 클릭하고 설정을 **Save**(저장)합니다.

EIGRP 고급 설정 구성

라우터 ID, 스텝 라우팅 및 인접성 변경 사항과 같은 EIGRP 고급 설정을 구성할 수 있습니다.

프로시저

- 단계 1 **EIGRP** 페이지에서 **Advanced**(고급) 탭을 클릭합니다.
- 단계 2 **Default Route Information**(기본 경로 정보) 아래의 EIGRP 업데이트에서 기본 경로 정보의 송수신을 제어할 수 있습니다.
- **Router ID (IP Address)**(라우터 ID(IP 주소)) - 외부 경로에 대한 원래 라우터를 식별하는 데 사용되는 ID를 입력합니다. 외부 경로가 로컬 라우터 ID와 함께 수신될 경우 그 경로는 무시됩니다.

이 문제를 방지하려면 라우터 ID에 대한 전역 주소를 지정합니다. 각 EIGRP 라우터에 고유한 값이 구성되어야 합니다.

- **Accept Default Route Info**(기본 경로 정보 수락) - 외부 기본 라우팅 정보를 수락하도록 EIGRP를 구성하려면 체크 박스를 선택합니다.
 - **Access List**(액세스 목록) — **Access List**(액세스 목록) 드롭다운에서 기본 경로 정보를 수신할 때 허용되는 네트워크와 허용되지 않는 네트워크를 정의하는 표준 액세스 목록을 지정합니다. 새 표준 액세스 목록 개체를 추가하려면 **Add**(추가) (+)을 클릭합니다. 자세한 절차는 [표준 ACL 개체 설정](#)의 내용을 참조하십시오.
- **Send Default Route Info**(기본 경로 정보 전송) - 외부 기본 라우팅 정보를 알리도록 EIGRP를 구성하려면 체크 박스를 선택합니다.
 - **Access List**(액세스 목록) — **Access List**(액세스 목록) 드롭다운에서 기본 경로 정보를 전송할 때 허용되는 네트워크와 허용되지 않는 네트워크를 정의하는 표준 액세스 목록을 지정합니다. 새 표준 액세스 목록 개체를 추가하려면 **Add**(추가) (+)을 클릭합니다. 자세한 절차는 [표준 ACL 개체 설정](#)의 내용을 참조하십시오.

단계 3 **Administrative Distance**(관리 거리)에서 다음을 지정합니다.

- **Internal Distance**(내부 거리)—EIGRP 내부 경로를 위한 관리 거리. 내부 경로는 동일한 자율 시스템 내의 다른 엔티티로부터 학습된 것입니다. 유효한 값의 범위는 1 ~ 255입니다. 기본값은 90입니다.
- **External Distance**(외부 거리)—EIGRP 외부 경로를 위한 관리 거리. 외부 경로는 자율 시스템의 외부에 있는 네이버로부터 최상의 경로가 학습된 경로입니다. 유효한 값의 범위는 1 ~ 255입니다. 기본값은 170입니다.

단계 4 **Adjacency Changes**(인접성 변경)에서 다음을 지정합니다.

- **Log Neighbor Changes**(인접한 라우터 변경 사항 기록) - EIGRP 인접한 라우터 인접성 변경 사항 로깅을 활성화하려면 확인란을 클릭합니다.
- **Log Neighbor Warnings**(인접한 라우터 경고 로깅) - EIGRP 인접한 라우터 경고 메시지 로깅을 활성화하려면 확인란을 클릭합니다.
- (선택 사항) 반복되는 인접한 라우터 경고 메시지의 시간 간격(초)을 입력합니다. 유효한 값의 범위는 1 ~ 65535입니다. 반복 경고가 이 간격 중 발생할 경우 로깅되지 않습니다.

단계 5 **Stub**(스텝) 아래에서 디바이스를 EIGRP 스텝 라우팅 프로세스로 활성화하려면 다음 EIGRP stub routing processes(EIGRP 스텝 라우팅 프로세스) 확인란 중 하나 이상을 클릭합니다.

- **Receive only**(수신만) - EIGRP 스텝 라우팅 프로세스가 인접한 라우터로부터 경로 정보를 수신 하되 인접한 라우터로 경로 정보를 보내지 않도록 구성합니다. 이 옵션을 선택하면 다른 stub 라우팅 옵션을 선택할 수 없습니다.
- **Connected**(연결됨) - 연결된 경로를 알립니다.

- **Redistributed**(재배포됨) - 재배포된 경로를 알립니다.
- **Static**(고정) - 고정 경로를 알립니다.
- **Summary**(요약) - 요약 경로를 알립니다.

단계 6 **Default Metrics**(기본 메트릭)에서 EIGRP 라우팅 프로세스로 재배포되는 경로의 기본 메트릭을 정의합니다.

- **Bandwidth**(대역폭) - 경로의 최소 대역폭(초당 킬로 비트)입니다. 유효한 값의 범위는 1 ~ 4294967295입니다.
- **Delay Time**(지연 시간) - 10마이크로초 단위의 경로 지연입니다. 유효한 값의 범위는 0~4294967295입니다.
- **Reliability**(신뢰성) - 패킷 전송의 성공률이며 0~255의 숫자로 표시됩니다. 값 255는 100% 신뢰성을 나타내고, 0은 신뢰성 없음을 의미합니다.
- **Loading**(로딩) - 경로의 유효 대역폭입니다. 유효한 값 범위는 1~255입니다. 255는 100% 로딩을 나타냅니다.
- **MTU** - 경로의 최대 전송 단위에 대해 허용되는 최소 값입니다. 유효한 값의 범위는 1 ~ 65535입니다.

EIGRP 기록

기능	버전	최소 Threat Defense	세부 사항
EIGRP 컨피그레이션	7.2	Any(모든)	이전 릴리스에서는 FlexConfig를 통해서만 위협 방어에서 EIGRP를 구성할 수 있었습니다. FlexConfig는 더 이상 EIGRP 구성을 지원하지 않습니다. 이제 관리 센터 UI에서 위협 방어에 대한 EIGRP 설정을 구성할 수 있습니다. 신규/수정된 화면: Devices (디바이스) > Device Management (디바이스 관리) > Routing (라우팅) > EIGRP

번역에 관하여

Cisco는 일부 지역에서 본 콘텐츠의 현지 언어 번역을 제공할 수 있습니다. 이러한 번역은 정보 제공의 목적으로만 제공되며, 불일치가 있는 경우 본 콘텐츠의 영어 버전이 우선합니다.